PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 17/60 — A1

(11) International Publication Number: WO 00/51039

(43) International Publication Date: 31 August 2000 (31.08.00)

(21) International Application Number: PCT/AU99/01173

(22) International Filing Date: 24 December 1999 (24.12.99)

(30) Priority Data:
PP 8933 26 February 1999 (26.02.99) AU

(71) Applicant *(for all designated States except US)*: ENSHRINE CA PTY LTD. [AU/AU]; KPMG Centre, 161 Collins Street, Melbourne, VIC 3000 (AU).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: WATSON, Robert, John [AU/AU]; 65 Alan Road, Berowra Heights, NSW 2082 (AU).

(74) Agent: FREEHILLS CARTER SMITH & BEADLE; MLC Center, Martin Place, Sydney, NSW 2000 (AU).

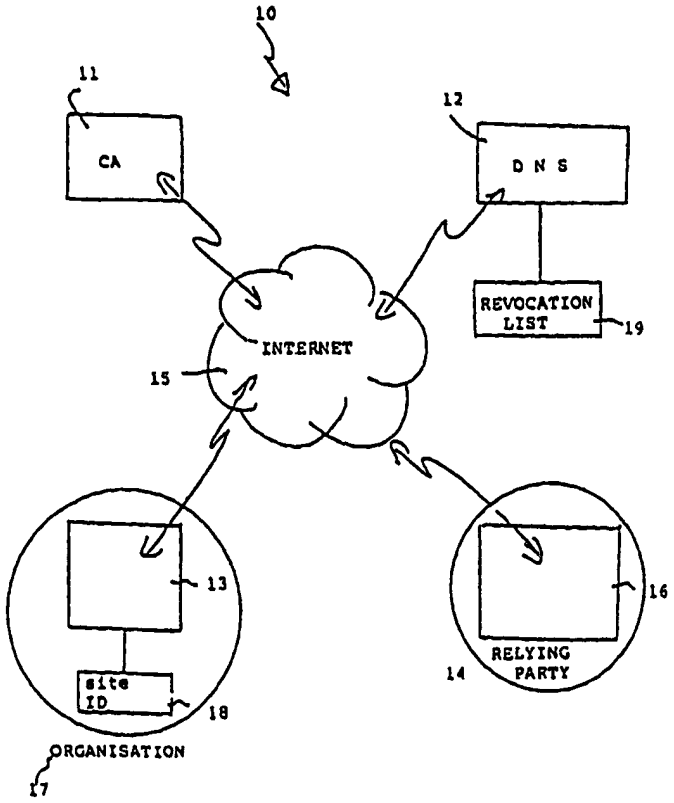
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: SITE CERTIFICATE SYSTEM

(57) Abstract

A site certificate system for use on the Internet (15) (as defined in the specification), said system comprising a certificate authority (11) adapted to issue site identifications (18) characteristic of a predetermined organisation (17), said certificate authority also being adapted to communicate with a domain name server registry (12) thereby to issue non–compliance notifications and a revocation list (19) for use by the domain name server registry so as to indicate to a relying party (14) that said predetermined organisation does not satisfy certain selected parameters; said selected parameters being under near continuous monitoring by said certificate authority.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

SITE CERTIFICATE SYSTEM

The present invention relates to a site certificate system and, more particularly, to such system adapted for rapid and timely maintenance of authentication status of a site certificate adapted particularly for use on what is commonly known as the "Internet".

BACKGROUND

The Internet may be described as a worldwide interconnection of computers all of which are adapted to communicate according to a common protocol currently the protocol is known as TCP/IP.

Communication between computers according to this protocol takes place across a multitude of communication channels including the public switch telephone network (PSTN) and also more restricted channels.

One problem with this form of communication system is that it can be difficult to ensure data integrity and confidentiality. Allied to this is the problem of identity of sources of data - that is how can a relying party be sure that the data it receives purporting to come from a particular computer site does, in fact, come from that site, come with the clear authority of the owner of the site, and, more particularly, that the owners of the site are who they purport to be.

A partial solution to this identity confirmation or authentication problem has come about by trusted third parties providing a secure electronic file which can be utilised to confirm site identity.

A problem with this arrangement is that the trusted third party which issues the site identification upon which other parties then rely may, itself, not always have up to date information as to the status and identity of the owners of the site in respect of which the site identification is issued.

It is an object of the present invention to address or alleviate this problem.

BRIEF DESCRIPTION OF INVENTION

The invention consists in a site certificate system for use on the Internet (as defined in the specification), said system comprising a certificate authority adapted to issue site identifications characteristic of a predetermined organisation, said certificate authority also being adapted to communicate with a domain name server registry thereby to issue a revocation notification to the domain name server registry and update a revocation list for use by the domain name server registry so as to indicate to a relying party that said predetermined organisation does not satisfy certain selected parameters;

said selected parameters being under near continuous monitoring by said certificate authority.

BRIEF DESCRIPTION OF DRAWINGS

One embodiment of the invention will now be described with reference to the accompanying drawing wherein:

Fig. 1 is a block diagram of a site certificate system according to a first embodiment of the invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENT

With reference to Fig. 1 there is shown, in block diagram form, components of a site identification system adapted to co-operate in accordance with a first embodiment of the invention.

The site certificate system 10 includes a Certificate Authority (CA) 11, a domain name server (DNS) 12, a first organisation server 13 and a relying party 14.

In this embodiment each of the sites 11, 12, 13, 14 is adapted to communicate over the Internet 15 by way of computer interface.

In use, a computer 16 of relying party 14 will place a query onto the Internet seeking the address of first organisation server 13. A domain name server 12 will match the name of the organisation 17 with an Internet address of

first organisation server 13 following which a data connection over Internet 15 will be established between

computer 16 of relying party 14 and first organisation server 13 of organisation 17.

As part of the establishment of the data connection the site identification 18 residing on first organisation server 13 will be interrogated by computer 16 for the purposes of:

1. Authenticating the identity of first organisation server 13; and

2. Providing an encryption key for the purposes of encrypting the data stream passing between computer 16 of relying party 14 and first organisation server 13 of organisation 17.

The site identification 18 is issued by certificate authority 11, the certificate authority 11 being a trusted third party.

Having interrogated the site identification 18 computer 16 of the relying party 14 may then proceed with data interchange over the Internet 15 between computer 16 and first organisation server 13 with a higher level of confidence than would otherwise be the case that:

1. First organisation server 13 is under the control and sponsorship of organisation 17; and

2. Data sent to and derived from first organisation 13

will not be able to be decoded by any other parties having access to the Internet 15.

In this embodiment certificate authority 11 maintains a near continuous monitoring of selected parameters pertaining to identity, ownership and financial status of organisation 17 whereby, should one or more of those parameters change in a way which would indicate that site identification 18 no longer reflects correctly the identity, ownership or financial status of organisation 17 then the certificate authority 11 lists the site identification 18 as no longer valid and takes steps to notify the domain name server 12 to re-route enquiries made over the Internet in relation to the domain name of first organisation server to a page which indicates that the site ID 18 of organisation 17 has been revoked. The revocation list 19 published by the certificate authority 11 resides on certificate authority 11. The domain name server may also redirect queries concerning organisation 17 to the computer upon which the revocation list 19 resides.

In this matter relying party 14 can be confident to a higher level than heretofore that a communication with first organisation server 13 over Internet 15 is a communication with a site which has the sponsorship and approval of organisation 17 and that organisation 17 is in a position to provide the sponsorship and/or approval with reference to the selected parameters which, in this

instance, comprise identity, ownership and financial status.

The above describes only one embodiment of the present invention and modifications, obvious to those skilled in the art, can be made thereto without departing from the scope and spirit of the present invention.

CLAIMS

1. A site certificate system for use on the Internet (as defined in the specification), said system comprising a certificate authority adapted to issue site identifications characteristic of a predetermined organisation, said certificate authority also being adapted to communicate with a domain name server registry thereby to issue non-compliance notifications and a revocation list for use by the domain name server registry so as to indicate to a relying party that said predetermined organisation does not satisfy certain selected parameters; said selected parameters being under near continuous monitoring by said certificate authority.

2. The site certificate system of Claim 1 wherein said selected parameters comprise one or more of identity, ownership and financial status.

3. The site certificate system of Claim 1 or Claim 2 wherein said step of near continuous monitoring comprises monitoring on a daily basis.

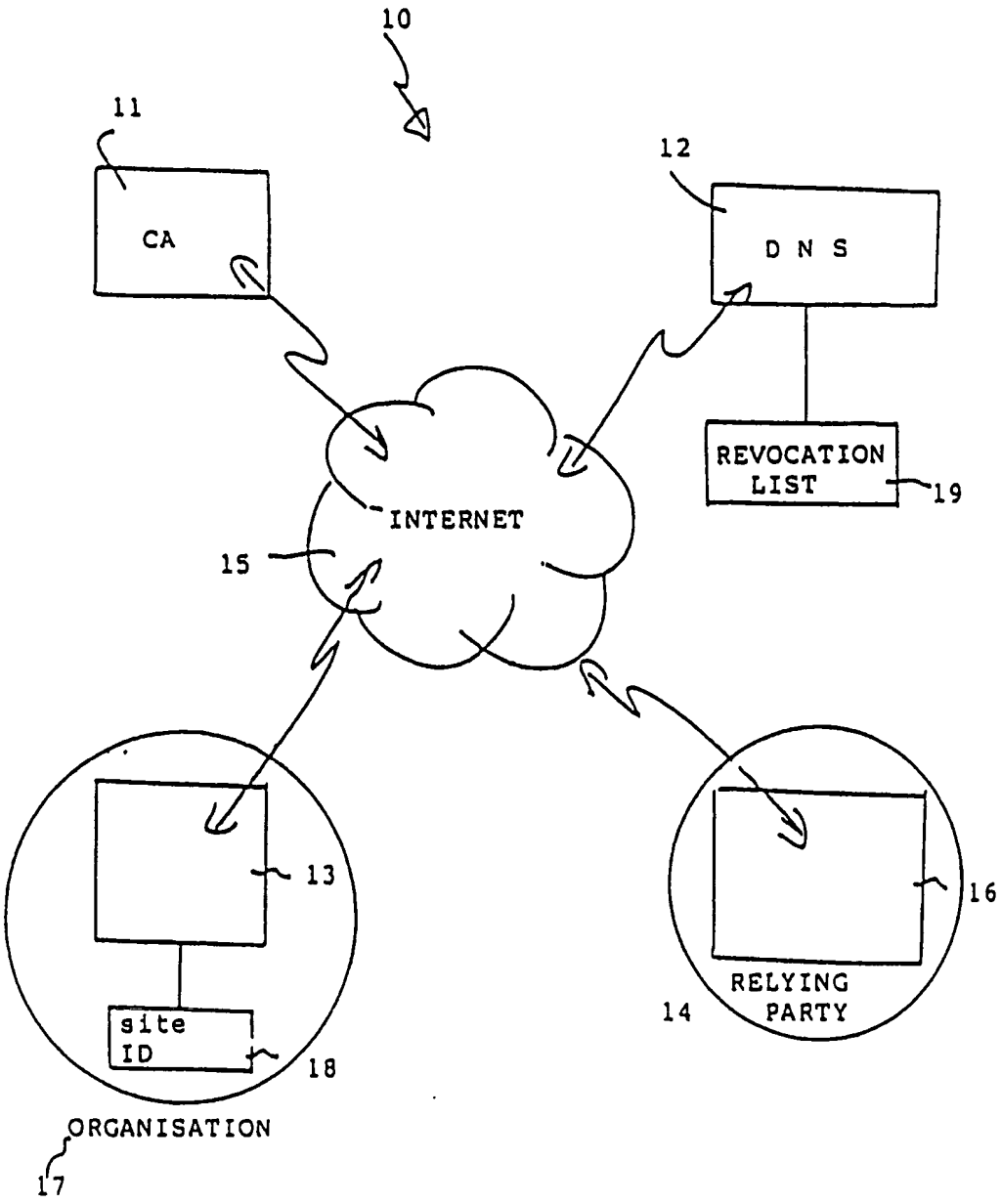

10
11
CA
12
D N S
REVOCATION LIST
19
INTERNET
15
13
site ID
18
ORGANISATION
17
RELYING PARTY
14
16

FIG. 1.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU 99/01173

A. CLASSIFICATION OF SUBJECT MATTER

Int Cl[7]: G06F 17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC: G06F 17/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WPAT: "site certificat:"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5850442 A (MUFTIC) 15 December 1998	
A	WO 98/37675 (VERIFONE, INC) 27 August 1998 Abstract	
A	WO 98/11716 (E-STAMP CORPORATION) 19 March 1998	
A	WO 98/09209 (INTERTRUST TECHNOLOGIES CORP) 5 March 1998 Abstract	

☐ Further documents are listed in the continuation of Box C

☐ See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 February 2000	16 FEB 2000
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	Authorized officer J.W. THOMSON Telephone No.: (02) 6283 2214